IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

PLAINTIFF'S BRIEF REGARDING TEXTUAL INTERPRETATION OF THE DATA ACCESS LAW

As the parties' joint submission filed on October 7, 2022, makes clear, Plaintiff Alliance for Automotive Innovation ("Auto Innovators") proposed alternative and practical interpretations of the Data Access Law whereas the Attorney General simply doubled down and repeated her litigation position about that law's meaning. Worse, the Attorney General refused to offer interpretations or even address important and practical questions about the law's language. As a result, the automotive industry remains faced with a law crafted with the intention to gain leverage over automakers—not because anyone thought it could be complied with safely, but rather to apply pressure on automakers in negotiations over data access. Automakers, however, cannot comply with a law that would render their vehicles unsafe and therefore noncompliant with federal legal obligations. Their efforts to work with the Attorney General to limit some of the law's harm have been unsuccessful. The law remains as dangerous as ever to Massachusetts' drivers.

The Data Access Law requires standardized access to electronic systems in all vehicles sold in the Commonwealth, with either no security at all or security run by a hypothetical third party. That third party does not exist, and the auto industry cannot establish and fund one given

the law's prohibition on their direct or indirect involvement in such an entity. At the same time that the law opens up broad access to highly sensitive vehicle systems, it directly forecloses Auto Innovators' original equipment manufacturer ("OEM") members from playing any meaningful role in protecting those systems. Every expert in this case agreed that immediate compliance with the technical requirements of the Data Access Law was impossible, and the evidence Auto Innovators presented at trial shows that, even with more time, there is no way to do so in a manner that is safe and maintains adequate cybersecurity.

Tellingly, the group that sponsored the Data Access Law realized its error and has taken a different approach in its latest initiative effort, in Maine. The Maine ballot language implicitly acknowledges a key flaw of the Data Access Law and attempts to correct it by requiring the Attorney General there to designate the independent third party; establishing a process and timeline to allow for industry input; and identifying specific International Organization for Standardization (ISO) standards to guide that effort through a structured, gradual implementation. *See* Maine Right to Repair Citizen Initiative §§ 2-3, https://www.repairerdrivennews.com/wp-content/uploads/2022/08/maine-R2R-legislation.pdf.[1]

Before discussing specific terms in the Massachusetts law, it is worth noting a few things at the outset:

First, the appropriate framework for assessing the Data Access Law's requirements is the text of the law itself. For statutory analysis, the First Circuit has consistently recognized that the plain language is the beginning, and often the end, of the matter. *See, e.g.*, *Whyte v. Lynch*, 807 F.3d 463, 471 (1st Cir. 2015) ("We therefore return, as we must, to the plain language of the statute."); *Sun Cap. Partners III, LP v. New Eng. Teamsters & Trucking Indus. Pension Fund*, 724

[1] To be sure, despite these corrections, there remain other, serious problems with the proposed Maine ballot initiative.

F.3d 129, 149 (1st Cir. 2013) ("We begin (and ultimately end) our analysis by reviewing the plain language of [the statutory provision]."); *Evans v. Akers*, 534 F.3d 65, 69 (1st Cir. 2008) ("As in any case of statutory construction, we begin our analysis with the plain language of the statute.").

Even when, with the benefit of hindsight, language in a statutory provision appears to be unusually broad or invite deleterious consequences, the plain text controls. *See, e.g.*, *Evans*, 534 F.3d at 75 (noting that "costs associated with [satisfying a statutory requirement] cannot alter our reading of the plain language of the statute itself"). Indeed, courts are not permitted to infer ambiguity in otherwise plain text even to avoid constitutional infirmities. *See, e.g.*, *Miller v. French*, 530 U.S. 327, 341 (2000) (noting that the "constitutional doubt canon does not give a court the prerogative to ignore the legislative will") (quotations omitted); *Salinas v. United States*, 522 U.S. 52, 60 (1997) ("We cannot press statutory construction to the point of disingenuous evasion even to avoid a constitutional question.") (quotations and brackets omitted). That the Data Access Law's provisions started as a ballot proposal also does not change the analysis. They are now codified into Massachusetts law. And, after all, plain-language review carries the day with all types of texts, even private contracts. *See, e.g.*, *AJC Int'l, Inc. v. Triple-S Propiedad*, 790 F.3d 1, 7 (1st Cir. 2015) (looking to the "plain language" of terms in an insurance policy).

Focusing on the plain language of the Data Access Law also accords with how Massachusetts courts would analyze the state statutory provisions at issue. The Supreme Judicial Court calls it a "fundamental tenant of statutory interpretation" that "statutory language should be given effect consistent with its plain meaning." *Boss v. Town of Leverett*, 484 Mass. 553, 557 (2020) (internal quotations omitted). Statutory language is to be interpreted according to its "ordinary language." *Commonwealth v. Daley*, 463 Mass. 620, 624 (2012). And the primacy of that approach extends to a refusal to read into statutory text new language that would narrow the

scope to make the breadth of a law more reasonable. *See, e.g.*, *Fernandes v. Attleboro Hous. Auth.*, 470 Mass. 117, 129, (2014) ("We do not read into a statute a provision which the Legislature did not see fit to put there, whether the omission came from inadvertence or of set purpose.") (internal quotations and brackets omitted).

Second, though the Attorney General's statutory construction could provide insights into her enforcement approach, it is not entitled to any special weight, particularly for any variance from the Data Access Law's plain text. Both Sections 2 and 3 of the law are self-executing, with nary any (public) attempt by the Attorney General to engage in agency regulations by issuing the required Section 4 notice or otherwise. *See* Mass. Const. amends. art. 48, pt. V, § 1. The "general rule" is "not to give deference to agency interpretations advanced for the first time in legal briefs." *Kisor v. Wilkie*, 139 S. Ct. 2400, 2417 n.6 (2019). Moreover, there is no reason to believe that the Attorney General would bring to bear any particular expertise on these matters, in contrast to a subject-matter expert like the National Highway Traffic Safety Administration ("NHTSA"). *See, e.g.*, *Souza v. Registrar of Motor Vehicles*, 462 Mass. 227, 229 (2012) (noting that the concept of agency deference is premised in part on "the agency's experience, technical competence, and specialized knowledge"; when an agency lacks "any special competence to determine what the [voters] meant" by a term "unrelated to the[] subjects" over which it has "specialized knowledge," "the interpretive question . . . is a purely legal one" for the Court). And, in any event, it is well-recognized that "no deference is due to agency interpretations at odds with the plain language of the statute itself." *Pub. Empl. Ret. Sys. of Ohio v. Betts*, 492 U.S. 158, 171 (1989).

Finally, much (though not all) of the disagreement between Auto Innovators and the Attorney General concerns means of compliance with the law rather than definitions of terms in the law itself. Once the parties have submitted additional affidavits, Auto Innovators intends to

discuss the issue of compliance more extensively. For now, Auto Innovators briefly addresses the issue only as it relates to matters the Attorney General raised in her submissions regarding textual interpretations of the Data Access Law. *See* II, *infra*. The point is simple: Even the Attorney General's favored interpretations would not eliminate the cybersecurity risks associated with an immediate attempt to comply with the Data Access Law.

I. The Plain Text of the Data Access Law Showcases Its Considerable Breadth.

A. Section 2

Section 2 sets out two disjunctive, alternative requirements. Manufacturers can comply with the law by designing and implementing an "authorization system for access to vehicle networks and their on-board diagnostic systems [that] is standardized across all makes and models sold in the Commonwealth and . . . administered by an entity unaffiliated with a manufacturer." Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)). Alternatively, manufacturers must make their on-board diagnostic systems "standardized" and accessible "without authorization by the manufacturer, directly or indirectly." *Id.* The parties dispute several terms.

1. As one method of compliance, Section 2 contemplates an independently administered "authorization system for access to *vehicle networks and their on-board diagnostic systems*" that is "standardized across all makes and models sold in the Commonwealth." Data Access Law § 2 (emphasis added). The plain language of the statutory provision thus encompasses not only "on-board diagnostic systems" but also "vehicle networks," of which on-board diagnostic systems are only a part. *Id.*

In its recent submission, the Attorney General elides the "vehicle networks" issue. Joint Submission (ECF No. 290) at 4. But the Attorney General has taken the position that "vehicle networks" does not include any electronic networks beyond those in a vehicle's on-board

diagnostic system. *See* Tr. Ex. 30 at 3 (interrogatory response). That interpretation makes no sense. If the drafters of Section 2 meant to target only "on-board diagnostic systems," there was no need to include the broader phrase. And "[i]t is a cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (internal quotations omitted). Moreover, no statutory canons of construction point the other direction. There is, for instance, no reason to believe that the phrase in Section 2 was "inadvertently inserted" or "repugnant to the rest of the statute." *Chickasaw Nat. v. United States*, 534 U.S. 84, 94 (2001) (quotations omitted). Nor are there any antecedents or consequents that would counsel reading the "and" between "vehicle networks" and "on-board diagnostic systems" as anything other than conjunctive. *See, e.g., Encino Motorcars, LLC v. Navarro*, 138 S. Ct. 1134, 1141 (2018).

2. The Attorney General continues to insist that Section 2 prohibits only manufacturer authorization, not manufacturer authentication, because authorization and authentication are separate. Joint Submission 6-7; *accord, e.g.*, Def.'s Post-Trial Proposed Findings of Fact and Conclusions of Law ("Def.'s PCOL"), ECF No. 232, at Def.'s PCOL ¶¶ 40-43. There is no basis, textual or otherwise, to decouple authentication from the statutory prohibition on OEM "authorization."

For one, it makes no sense to read "authorization" as distinct from "authentication." Authentication is an important aspect of authorization. June 14 Tr. at 211:3 (Bort). Authorization deals broadly with the entire scope of access—*e.g.*, how many and which doors a key can open—while authentication deals more narrowly within authorization by identifying the unique person who would get the key to access particular doors. *See id.* at 210:14-211:1 (Bort). Any ability to

authenticate users to change entire vehicle systems without the ability to authorize users in the first place would be meaningless—and dangerous. *Id.* at 211:6-8 (Bort).

Moreover, treating authorization as encompassing authentication accords with understanding in the technology industry. Courts routinely observe that, so long as it accords with the plain text, undefined terms that are specific to a particular industry should be given a meaning consistent with their industry usage. *E.g., Consolidated Cos., Inc. v. Lexington Ins. Co.*, 616 F.3d 422, 430 (2010) (holding that industry term in text "should be construed" "in light of the customs and usages of the industry"); *see also Verrill Farms, LLC v. Farm Family Casualty Ins. Co.*, 86 Mass. App. Ct. 577, 587-88 (2014) (discussing *Consolidated Cos.*). The Attorney General urged this Court to "'take note of terms that carry technical meaning[s],' including 'when interpreting a statute about computers.'" Def.'s Mot. for Judgment as a Matter of Law (ECF No. 204) at 4 (quoting *Van Buren v. United States*, 141 S. Ct. 1648, 1657 (2021)). And the very Supreme Court decision on which the Attorney General relied for that proposition dealt with this issue. The Court in *Van Buren* recognized that the concept of "authorized access" "contemplates *a specific type of authorization*—that is, *authentication*, which turns on whether a user's credentials allow him past a computer's access gate." *Van Buren*, 141 S. Ct. at 1659 n.9 (internal quotations omitted). That is, the technical understanding of authorization in the computing world subsumes a process of authenticating a user to grant access. *Id.* (noting that *A Dictionary of Computing* defines "'authorization' as a 'process by which users, having completed an . . . authentication stage, gain or are denied access to particular resources based on their entitlement'").

Even the Attorney General's own expert disagrees with her narrow interpretation of "authorization." At trial, Mr. Romansky repeatedly observed that by removing OEMs' ability to authorize users, Section 2 also removes OEMs' ability to authenticate users—meaning the ability

to decide who can do what to their vehicles. *See, e.g.*, Romansky Aff. ¶ 28 ("Vehicles that fully comply with the 2020 Right to Repair Law will need to support authentication and authorization of a broad array of different users and diagnostics tools."); June 16 Tr. at 44:14-18 (Romansky) ("I think section 2 establishes a common authentication authorization mechanism[.]"); June 15 Tr. at 193:24-194:6 (Romansky) (agreeing that both of his proposed theoretical solutions to Section 2 involve having authentication services provided by an independent organization).

3. Finally, Section 2 again speaks in sweeping terms when it mandates both standardization across all makes and models sold by all OEMs in the Commonwealth (and not just within each OEM) and proscribes "*any* authorization by the manufacturer, directly *or indirectly*" to on-board diagnostic systems, unless there is standardized access to all vehicle networks across all vehicles sold in the Commonwealth and controlled by a third-party entity, which would seemingly require all automakers to tailor technology to one system. Data Access Law § 2 (emphasis added). In cybersecurity terms, that is a recipe for disaster because it creates a single point of attack for all vehicles in Massachusetts. Diversity of attack surface is a basic tenet of good cybersecurity practices. Trial Ex. 3 (NHTSA Cybersecurity Guidance) at 6.74-6.78. As it stands, a hacker seeking to control a particular OEM's vehicles has to go car-by-car. Access to one car would not yield access to other cars. But the law changes all that and puts all security keys into the hands of a single, yet-to-be-established party that, if hacked, could lead to access to all vehicles in Massachusetts. Given the potentially dire consequences, car companies simply cannot take that risk and still comply with their federal-law safety and emissions obligations.

Worse, the third-party entity is a prerequisite to being able to comply with the Data Access Law, as OEMs would have to tailor their systems around that entity's technology. That entity does not exist. And at least according to the Attorney General, it cannot be affiliated in any way—

formally, informally, or contractually—with the OEMs. *See* Joint Submission 7. Accordingly, OEMs cannot create and fund this third-party entity, as that would violate the law's prohibition on their direct involvement.[2] Unlike the Maine initiative, which requires the Attorney General to establish this entity and creates a theoretical mechanism for third-party authorization, *see* Maine "Right to Repair" Citizen Initiative § 2, the Data Access Law is dangerously silent on this key issue. Compliance with Section 2 through such an unaffiliated third party cannot even begin to be contemplated until that third-party entity is set up and can assure the auto industry of its safety.

B. Section 3

Section 3 requires OEMs to create an "inter-operable, standardized, and open access" "platform" beginning in model year 2022 vehicles. Data Access Law § 3. That platform also must be "[d]irectly accessible by the owner through a mobile-based application." *Id.* It must be "[c]apable of securely communicating all mechanical data emanating directly from the motor vehicle via a direct connection to the platform," *id.*—where "mechanical data" is broadly defined to include "any vehicle-specific data, including telematics systems data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle," *id.* § 1. If the vehicle owner authorizes it, the "mechanical data" emanating from this novel platform must be "directly accessible" to an independent repair facility for the time needed to maintain, diagnose, and repair the vehicle. *Id.* § 3. And that "access" must be provided on both a read and write basis—so that users will have "the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." *Id.*

[2] The "ordinary meaning" (*Penobscot Nat. v. Frey*, 3 F.4th 484, 491 (1st Cir. 2021)) of "indirectly" includes any "way that is not direct or not connected in a simple way." Cambridge English Dict., *available at* https://dictionary.cambridge.org/us/dictionary/english/indirectly. And the phrase "directly or indirectly" (Data Access Law § 3) is commonly understood to be a "broad" prohibition. *Burley v. Comets Cmty Youth Ctr., Inc.*, 75 Mass. App. Ct. 818, 821 (2009) (quoting *N. Am. Expositions Co. Ltd. P'ship v. Corcoran*, 452 Mass. 852, 862 (2009)).

1. In its portion of the joint submission, Auto Innovators noted its concern that by including data "otherwise related" to data needed to maintain, diagnose, and repair a vehicle, Section 3 required access—transmissible via mobile app no less—to virtually all data generated by vehicles. Joint Submission 13. Rather than address or grapple with that reality, the Attorney General simply parroted the statutory definition without considering that definition's individual terms. *Id.* By its plain terms, "mechanical data" is broader than that merely *used* for diagnosis, repair, or maintenance. The statutory definition applies to data "used for *or otherwise related to* the diagnosis, repair or maintenance of the vehicle." Data Access Law § 1 (emphasis added). The language after the disjunctive "or" must have some independent meaning. After all, it has long been the case, in Massachusetts as elsewhere, that "none of the words of a statute is to be regarded as superfluous." *Commonwealth v. Woods Hole, Martha's Vineyard and Nantucket S.S. Auth.*, 352 Mass. 617, 618 (1967) (internal quotations and alterations omitted); *accord TRW*, 534 U.S. at 31. Moreover, courts confronted with the term "otherwise related to" in other contexts have observed that the effect is to create a "broadly worded" obligation that extends beyond the terms directly modified by that language. *E.g.*, *Khan v. Parsons Glob. Servs., Ltd.*, 521 F.3d 421, 423 (D.C. Cir. 2008) (discussing an "otherwise related to" arbitration clause).

A limited reading of "mechanical data" would also render Section 2 superfluous in light of other, preexisting provisions of Chapter 93K. That chapter already requires OEMs to provide access to all data necessary for diagnosis, repair, or maintenance. *See* Mass. Gen. Laws ch. 93K, § 2(d)(1) (2013 Right to Repair Law); Potter Aff. ¶¶ 10-11; Tierney Aff. ¶ 78. By its plain terms, then, Section 2 of the Data Access Law expands the scope of Chapter 93K to a larger universe of vehicle data, which includes, but is not limited to, the data strictly necessary for diagnosis, repair, or maintenance.

In any event, even if the "otherwise related to" language were read out of the statute entirely, access to data necessary for "diagnosis, repair or maintenance" on the other conditions established in the Data Access Law would itself broadly entail access to potentially every electronic system in the vehicle. *Contra* Joint Submission 13-14. As NHTSA explained, "[b]ecause all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, [the] requirement [to provide access to 'mechanical data'] effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration." U.S. Statement of Interest (ECF No. 202) at 7.

2. The term "open-access platform" is not defined in the law. The Attorney General interprets "open access" to allow the use of OEM "security controls to ensure the safety and privacy of the consumer." Joint Submission 12; *accord* Defs.' Post-Evidence Memo. (ECF No. 217) at 6. But nothing in that term suggests that OEMs could continue to play that role. Tellingly, the new Maine initiative omits that problematic term altogether. *See* Maine "Right to Repair" Citizen Initiative § 3. After all, as commonly understood in the technical field, "open access" denotes "without restriction." *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1100-01 (N.D. Cal. 2015) (quoting *Opperman v. Path, Inc.*, 2014 WL 1973378, at *21 (N.D. Cal. May 14, 2014)). That is also NHTSA's studied judgment of what the law contemplates. *See, e.g.*, U.S. Statement of Interest 8 ("[T]he Data [Access] Law effectively requires open remote access, potentially accessible by anyone, to all of a motor vehicle's telematics systems."). As the United States noted, "open access must 'include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics, and repair'"—encompassing potentially any part of a vehicle. *Id.* at 7-8 (quoting Data Access Law § 3).

Nor would it make sense to decouple the "open access" requirement in Section 3 from the no-manufacturer-authorization access requirement in Section 2. It is a basic canon of statutory construction that related statutory provisions should be read to work together, not (as the Attorney General would have it) at odds with each other. *See, e.g., FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133, (2000) (observing that courts "interpret the statute as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into a[ ] harmonious whole") (quotations omitted); *In re Plaza Resort at Palmas, Inc.*, 741 F.3d 269, 277 (1st Cir. 2014) ("Statutes should be treated as a harmonious whole, and should be read together and not construed as divorced from their provisions.") (citation omitted). "Reading Sections 2 and 3 of the Data Access Law together," it is plain that "a motor vehicle manufacturer may not implement controls over remote access to any systems . . . unless those controls are administered by an unaffiliated third party." U.S. Statement of Interest 8. Certainly that is the reading that the law's proponents would adopt.

3. For "directly accessible," the Attorney General fails to grapple fully with the statutory language that this direct access includes specific access requirements for the user, including the ability to "send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair," Data Access Law § 3. *See* Joint Submission 14. The statutory language necessarily contemplates more than the user not needing to go "through the OEM to perform diagnosis, maintenance and repair." *Id.* By its plain terms, the "inter-operable, standardized and open access platform" itself (1) "shall be directly accessible by the owner of the vehicle through a mobile-based application"; (2) "upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility"; (3) and this access "shall include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." Data Access Law § 3.

4. As for the "ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair" term itself, both parties agree that this encompasses the ability to write data to vehicle systems. *See* Joint Submission 15. But the Attorney General goes on to insist that this "does not require access to write data to any vehicle component." *Id.* That makes no sense. Vehicle maintenance, diagnostics, and repair could well encompass any part of the vehicle. Thus, the ability to write data as part of maintenance, diagnostics, and repair necessarily entails wide-ranging access. Again, NHTSA understands that reality. U.S. Statement of Interest 7 ("Because all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, [the] requirement [to provide access to "mechanical data"] effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration.").

5. To justify one of its workaround "solutions" to Section 3, the Attorney General proffers an implausible definition of "mobile-based application" by which a dongle *permanently affixed to the vehicle* would qualify as "mobile." Joint Submission 15. A stationary dongle is the opposite of a mobile-based application. By contrast, accessibility via a mobile phone accords with the plain meaning of "mobile," which means "able to be moved from one place to another" and is "used to describe a service available on a cell phone, small computer, etc." Cambridge English Dict., *available at* https://dictionary.cambridge.org/us/dictionary/english/mobile.

Moreover, the Attorney General's crabbed definition of "mobile" is not how Section 3 was sold to Massachusetts voters. They were told that the information would go to their smart phones. *See* Ex. 509 at 4 ("Owners of motor vehicles with telematics systems would get access to mechanical data through a mobile device application."). And that is how the ballot proposals' drafters understood it to work, too. *See* June 15 Tr. 29:12-22 (Lowe) (explaining that the data must

go directly from the vehicle to the owner's smartphone). Unsurprisingly, the Attorney General's witnesses conceded that there is not a readily available "mobile-based application" (Data Access Law § 3) to comply with the law. June 15 Tr. at 95:21-96:17 (Potter); *id.* at 126:13-15 (Smith).

6. Finally, the Attorney General strains to remove the possibility of cybersecurity issues by proposing to graft onto the term "securely communicating" the notion that the sender and the recipient must first be authenticated before the secure communication takes place, which (according to the Attorney General) would define away any cybersecurity concerns. Joint Submission 13. It is, however, well-established that "[a] court may not add words to [the] statute that the Legislature did not put there." *Sunshine Lady Found., Inc. v. Rozek ex rel. Doris Buffett Revocable Tr.*, 2021 WL 9059746, at *4 (D. Mass. 2021) (quoting *Bank of Am., N.A. v. Rosa*, 466 Mass. 613, 618 (2013)). There is no reason to believe that the Data Access Law's drafters intended that term somehow to immunize other provisions in the statute from cybersecurity scrutiny.

II. Even Under the Attorney General's Interpretation, Manufacturers Could Not Safely Comply with the Data Access Law.

The Attorney General included throughout her submission statements suggesting that OEMs could safely and securely comply with Sections 2 and 3. *See, e.g.*, Joint Submission 4 (averring that OEMs can comply in a "way that does not compromise cybersecurity and which can be implemented in a timely manner"). Although Auto Innovators contemplates further briefing specifically focused on compliance, it responds here for the limited purpose of showing that even under the Attorney General's preferred construction, OEMs have no means of safely complying with the Data Access Law without introducing significant cybersecurity risks irreconcilable with their federal-law obligations.

As discussed, Section 2 of the Data Access Law requires one of two things: Either manufacturers must design and implement an "authorization system for access to vehicle networks

and their on-board diagnostic systems [that] is standardized across all makes and models sold in the Commonwealth and . . . administered by an entity unaffiliated with a manufacturer." Data Access Law § 2. Or manufacturers must immediately make on-board diagnostic systems "standardized" and accessible "without authorization by the manufacturer, directly or indirectly." *Id.* Either way—whether under the plain text of Section 2 or the Attorney General's preferred construction—manufacturers are cut out of the process of protecting access to their on-board diagnostic systems.

The first avenue for immediate compliance is a non-starter. It is undisputed that there is currently no "entity unaffiliated with a manufacturer" that could run a standardized authorization system that works on all makes and models sold in the Commonwealth by every OEM, Data Access Law § 2. *See, e.g.*, June 15 Tr. at 118:11-13 (Smith); *id.* at 96:18-25 (Potter); *id.* at 13:13-15 (Lowe) ("All along you knew that the third-party entity that is referenced in section 2 does not exist today?" // "Yes."); *accord, e.g.*, U.S. Statement 8 ("[T]he United States is not aware of any such third party that currently exists, or one that could likely be offered, operationalized, and scaled up to meet the Data Access Law's requirements in the necessary timeframe.").[3] Nor could OEMs themselves create and fund such an entity, as that would violate the prohibitions on their direct or indirect involvement in it.

Thus, the only option for immediate compliance with Section 2 would be the second path, which would require OEMs to "standardize[]" their on-board diagnostic systems across not just an OEM's vehicles but all vehicles sold by any OEM in the Commonwealth and make them accessible

[3] It was also undisputed at trial that there was no "authorization system for access to vehicle networks and their on-board diagnostic systems" that is "standardized across all makes and models sold in the Commonwealth." Data Access Law § 2. *See, e.g.*, June 15 Tr. 24:24-25-15 (Lowe); *id.* at 96:18-97:3 (Potter). Despite that, Section 2 was crafted to take effect just one month after voter approval and, by operation of Massachusetts law, applies to all vehicles model year 2018 and newer. *See* Mass. Const. amends. art. 48, pt. V, § 1.

"without authorization by the manufacturer, directly or indirectly." Data Access Law § 2. Again, the Attorney General's witnesses agreed. *See, e.g.,* June 15 Tr. at 26:13-17 (Lowe) ("[U]nder section 2, Mr. Lowe, either the manufacturer does not require any authorization at all or, if it does, the access has to be standardized and administered by a third party, right?" // "Correct."); *id.* at 118:11-13, 125:6-9 (Smith) (agreeing that immediate compliance with Section 2 is impossible); *id.* at 185:23-186:8 (Romansky) (expressly declining to opine on the first prong of Section 2).

As the evidence submitted at trial shows, to comply with Section 2 of the Data Access Law by standardizing access to on-board diagnostic systems, "without authorization by the manufacturer, directly or indirectly," Data Access Law § 2, OEMs would have to abandon their existing cybersecurity controls that protect safety- and emissions-critical functions, and thus help to ensure the safe operation of vehicles within prescribed emissions limits. Indeed, OEMs would have to completely upend their secure data access practices, opening the gates to their on-board diagnostic systems immediately. *E.g.*, June 14 Tr. at 70:6-14, 71:18-72:3, 73:14-22 (Tierney); Chernoby Aff. ¶ 65; Tierney Aff. ¶¶ 13, 90. Auto Innovators previously discussed some of the key cybersecurity controls that GM and FCA would have to remove. *See* Pl.'s Pre-Argument Br. (ECF No. 215) at 7-9. Each of Auto Innovators' members would have to do likewise. *See, e.g.*, Bort Aff. ¶ 93; Garrie Aff. ¶ 64. The Attorney General's repeated claim about Toyota remains incorrect. *See* Joint Submission 5. As made clear at trial, though Toyota does not employ a secured gateway, it has plenty of other cyber protections and access controls. *See* Pl.'s Pre-Argument Br. 7 n.9 (discussing, under seal, some of Toyota's practices).

With regard to Section 3, there is no "inter-operable, standardized, and open access" "platform" that allows users to access "vehicle mechanical data." Data Access Law § 3.[4] When the

[4] The requirement is pegged to MY2022 vehicles—which have long since rolled off the lot. *E.g.*, Tierney Aff. ¶¶ 7-8 (noting, at the time of trial, that model year 2022 vehicles were currently in production and their electric architecture

Court asked whether OEMs could provide the inter-operable, standardized, open access platform required by Section 3, *every* expert—both Auto Innovators' and the Attorney General's—agreed that OEMs could not. *See, e.g.*, June 16 Tr. at 41:21 (Smith) ("Definitely not right away."); *id.* at 42:1-3 (Romansky) ("I think the elements of a solution are available, but they're not assembled, and that has not been proven to all work together."); June 15 Tr. at 198:24-199:2 (Romansky) ("I'm not aware of any [telematics systems] that fully comply with Section 3, correct."); June 16 Tr. at 42:7-8 (Bort) ("I don't think we can do that right now."); *id.* at 42:10 (Garrie) ("I agree with my colleagues."). And in her recent submission, the Attorney General concedes that the "creation of a fully telematic platform will require time to design, test, and validate." Joint Submission 10.

The Attorney General suggests that the creation of the required platform can be speeded along through Secure Vehicle Interface ("SVI"). Joint Submission 11. But as Auto Innovators has explained, SVI is of no help to OEMs for anything approaching immediate, safe compliance with the Data Access Law. *See, e.g.*, Pl.'s Pre-Argument Br. 19; Pl.'s Post-Trial Proposed Findings of Fact ("Pl.'s PFOF") and Conclusions of Law ("Pl.'s PCOL"), ECF No. 233, at Pl.'s PFOF ¶ 131. SVI is a theoretical set of standards that has never been tested, confirmed, or deployed at scale. June 14 Tr. at 79:2-8 (Tierney); Bort Aff. ¶ 111-12. When the Data Access Law's proponents met with NHTSA to propose an SVI solution, NHTSA declined to endorse it on the grounds that "the establishment of a certificate authority would be extremely difficult and, in their opinion, likely not possible." Tr. Ex. 64; *see also* June 15 Tr. at 34:5-13 (Lowe).

In place of the platform specifically contemplated by Section 3, the Attorney General offers up instead a truncated version of previously discussed workarounds. The Attorney General claims

design was completed over two years before that). Indeed, given production timing, Section 3's requirements were set to take *retroactive* effect on the date the Data Access Law passed. *See, e.g.*, *id.*; June 15 Tr. at 51:14-17 (Lowe) (discussing business plan noting that automakers lock in the design of a production model three to five years before release).

that OEMs could provide a platform via an enhanced dongle plugged into the J-1962 connection port. Joint Submission 10. Even putting aside that a permanently affixed dongle cannot be conceived of as a "mobile-based application," *see* p. 13, *supra*, an enhanced dongle is not a viable solution for immediate, safe compliance with Section 3. *See* Pl.'s Pre-Argument Br. 15-17; Pl.'s PFOF ¶ 140. No dongle with that kind of functionality exists. June 15 Tr. at 120:8-10 (Smith). And dongles bring their own cybersecurity risks: the expert who floated the hypothetical dongle "solution" conceded that he has used simpler dongles to hack vehicles. *Id.* at 117:20-118:2 (Smith).

The Attorney General again suggests disabling telematics systems as a means of avoiding the requirements of Section 3. Joint Submission 10-11. But disabling telematics is a far different thing than complying with the law by developing and deploying an "inter-operable, standardized, and open access [telematics] platform." Data Access Law § 3. Among other problems with that "solution," preemption analysis assumes compliance with the law and statutory avoidance is not statutory compliance. *See, e.g.*, Pl.'s Pre-Argument Br. 13-14; Pl.'s PCOL ¶ 84. Voters were not told that a vote for the Data Access Law would mean requiring OEMs to stop selling vehicles in the Commonwealth with telematics systems because there is no way to comply with the law's requirements for such systems.

Thus, as with Section 2, there is no immediate path to safe compliance with Section 3. Any attempt to comply immediately with the requirement to deploy an "open access" regime for vehicle "mechanical data" (Data Access Law § 3) would require OEMs to remove or disable the same cybersecurity controls that protect safety- and emissions-critical vehicle functions. *See, e.g.*, June 14 Tr. at 72:4-17 (Tierney); Tierney Aff. ¶¶ 90, 99; June 14 Tr. at 126:20-127:10 (Chernoby); Bort Aff. ¶ 78; Garrie Aff. ¶ 90.

The unrealistic requirements and timeline in the Data Access Law substantially increases the risk of system hacks with potentially disastrous consequences. Without a manufacturer (or the unaffiliated third party that does not yet exist) to control authorization, anyone with access to a vehicle and sufficient technical know-how could write compromising data to the vehicle. Bort Aff. ¶ 90. And with OEM cybersecurity controls removed, hackers would have free rein to take remote control of vehicles—taking command, for instance, of a vehicle's brakes or its steering wheel. *E.g.*, Garrie Aff. ¶¶ 90, 96-97; Tierney Aff. ¶ 104; *see also* June 14 Tr. at 118:14-18 (Baltes) ("from a cyber perspective . . . it really broadens the attack [surface] on the vehicle.").

Indeed, nearly every vehicle on the road would be vulnerable to cyberattack if the Data Access Law went into effect. *See, e.g.*, June 14 Tr. 70:6-21, 71:18-72:3, 73:14-22 (Tierney) (explaining how compliance with the Data Access law would require removal of critical GM functions that protect against cyberattacks); June 14 Tr. 200:20-201:8 (Bort) ("[I]nherently, compliance requires the abrogation of the protections that have been built into them that have just been layered and built up over time" to protect against cyberattacks); Garrie Aff. ¶ 64 ("To comply with the Data [Access] Law, OEMs would have to remove or alter critical cybersecurity controls, which would substantially increase the safety risks of using their vehicles."); *accord* June 15 Tr. 113:3-21 (Attorney General's expert Smith) (confirming that "the Data Access Law would require OEMs to make changes to the cybersecurity they have on their vehicles today"; that "altering cyber protections that exist on a vehicle could make them more vulnerable to cyberattacks"; that "with the correct access, hackers can take over core functionality of a vehicle"; and that hackers could "thwart safety systems or install malware on a vehicle," among other possibilities). In an era where cyberattacks are increasing and government officials of all kinds are encouraging greater cybersecurity protections, the Data Access Law goes the opposite way.

Finally, it is not just OEMs sounding the alarm. The United States filed a statement of interest on behalf of NHTSA to call out—repeatedly—how immediate compliance with the Data Access Law's requirements would open up vehicles to cyberattack and threaten public safety. The predictable effect of taking the actions required under the Data Access Law, NHTSA explained, would be to "create serious safety problems for motor vehicle owners," by making it easier to hack into vehicle functions and "cause a severe crash, potentially leading to deaths or serious injuries." U.S. Statement at 6; *id.* at 8 ("[T]he Data [Access] Law requires motor vehicle manufacturers to take actions that potentially pose serious cybersecurity risks by opening uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing implementations. Such access could allow a hacker operating remotely to access these vehicle functions, and cause a severe crash, potentially leading to deaths or serious injuries."); *id.* at 9 ("The open access effectively required by the Data [Access] Law . . . has the potential to cause serious safety problems for motor vehicle owners and to frustrate the ability of motor vehicle manufacturers to follow their obligations to ensure vehicle safety.").

CONCLUSION

For the foregoing reasons, and those in Plaintiff's substantive briefing, Plaintiff respectfully requests that the Court (1) find in its favor on Counts I and II of its Complaint; (2) declare that the Data Access Law is unenforceable as preempted by federal law and/or invalid under the Due Process Clause; (3) permanently enjoin enforcement of the Data Access Law; and (4) grant any such further relief as the Court deems appropriate.

Dated: October 14, 2022

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Laurence A. Schoen

Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
MINTZ, LEVIN, COHN, FERRIS,
GLOVSKY, AND POPEO, P.C.
One Financial Center
Boston, MA 02111
Tel: (617) 542-6000
lschoen@mintz.com
eflynn-poppey@mintz.com

John Nadolenco (*pro hac vice*)
Erika Z. Jones (*pro hac vice*)
Jason D. Linder (*pro hac vice*)
Daniel D. Queen (*pro hac vice*)
Eric A. White (*pro hac vice*)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
jnadolenco@mayerbrown.com
ejones@mayerbrown.com
jlinder@mayerbrown.com
dqueen@mayerbrown.com
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice*)
Jessica L. Simmons (*pro hac vice*)
ALLIANCE FOR AUTOMOTIVE INNOVATION
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and that paper copies will be sent to those indicated as non-registered participants on October 14, 2022.

/s/ Laurence A. Schoen
Laurence A. Schoen